EB80-IR-07.012



MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

INSTRUÇÕES REGULADORAS DO SISTEMA DE GESTÃO ARQUIVÍSTICA E DOCUMENTAL DO EXÉRCITO (SIGADEx)

1ª Edição
2025

EB80-IR-07.012



MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

INSTRUÇÕES REGULADORAS DO SISTEMA DE GESTÃO ARQUIVÍSTICA E DOCUMENTAL DO EXÉRCITO (SIGADEx)

1ª Edição
2025

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

PORTARIA - DCT/C Ex Nº 073, DE 22 DE SETEMBRO DE 2025.

EB: 64202.002391/2025-70

Aprova as Instruções Reguladoras do Sistema de Gestão Arquivística e Documental do Exército (EB80-IR-07.012), 1ª Edição, 2025.

O CHEFE DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA, no uso da competência que lhe confere o art. 20 da Política de Gestão Documental do Exército Brasileiro, aprovada pela Portaria do Comandante do Exército nº 1.878, de 30 de novembro de 2022, e de acordo com o que consta do Processo Administrativo nº 64202.002391/2025-70, resolve:

Art. 1º Ficam aprovadas as Instruções Reguladoras do Sistema de Gestão Arquivística e Documental do Exército (SIGADEx) (EB80-IR-07.012), que com esta baixa.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

General de Exército HERTZ PIRES DO NASCIMENTO
Chefe do Departamento de Ciência e Tecnologia

(Publicado no Boletim do Exército nº 3, de 16 de janeiro de 2026)

FOLHA DE REGISTRO DE MODIFICAÇÕES (FRM)

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA

ÍNDICE DE ASSUNTOS

		Art.
PREFÁCIO		
CAPÍTULO I	DA FINALIDADE …………………………………………………………………………………	1º
CAPÍTULO II	DA ARQUITETURA DO SISTEMA	
Seção I	Da concepção do sistema …………………………………………………………………	2º/7º
Seção II	Da estrutura do sistema ……………………………………………………………………	8º
Seção III	Das atribuições ………………………………………………………………………………	9º/14
CAPÍTULO III	DO SISTEMA INFORMATIZADO	
Seção I	Da conceituação ………………………………………………………………………………	15
Seção II	Dos objetivos …………………………………………………………………………………	16
Seção III	Das fases do desenvolvimento e operação ………………………………………	17
Seção IV	Das fases do desenvolvimento …………………………………………………………	18
Seção V	Das fases da operação ………………………………………………………………………	19
Seção VI	Da proteção cibernética ……………………………………………………………………	20/24
Seção VII	Das assinaturas ………………………………………………………………………………	25/28
Seção VIII	Da digitalização de documentos físicos ………………………………………………	29
CAPÍTULO IV	DO REPOSITÓRIO DIGITAL CONFIÁVEL	
Seção I	Da conceituação …………………………………………………………	30
Seção II	Do planejamento para implantação ……………………………………	31
GLOSSÁRIO		

CAPÍTULO I
DA FINALIDADE

Art. 1º Estas Instruções Reguladoras (IR) têm por finalidade:

I - descrever as partes componentes do Sistema de Gestão Arquivística e Documental do Exército (SIGADEx), no âmbito do Exército Brasileiro (EB);

II - orientar a gestão dos referidos componentes integrantes do Sistema por seus atores envolvidos: usuários, administradores de sistema e técnicos de suporte e manutenção; e

III - delinear a arquitetura tecnológica do SIGADEx, com o mapeamento das estruturas organizacionais envolvidas, dos processos e dos agentes encarregados pela operação e manutenção desse sistema.

CAPÍTULO II
DA ARQUITETURA DO SISTEMA

Seção I
Da concepção do sistema

Art. 2º O Sistema de Protocolo Eletrônico de Documentos (SPED), o software do Módulo Integrador (MI) e os equipamentos infraestrutura de telemática são os componentes do SIGADEx.

Art. 3º A arquitetura proposta possui característica cliente-servidor, de forma distribuída, para atender aos usuários das Organizações Militares (OM) por meio de instâncias do SPED dedicadas. Estas instâncias são conectadas entre si via MI que será encarregado de orquestrar o trâmite de documentos e processos de forma automática.

Art. 4º O SPED é o módulo que se destaca por apresentar-se como a interface entre os usuários e o SIGADEx como um todo. É o componente de software responsável pela gestão eletrônica da produção documental.

Parágrafo único. O SPED é o Sistema Gestor Arquivístico e Documental (SIGAD) para uso administrativo no âmbito do EB.

Art. 5º O MI é o componente de software responsável pela integração entre as instâncias de SPED para troca de documentos. É o módulo responsável pela comunicação com os demais sistemas de gestão documental dos demais órgãos da Administração Pública Federal por meio do Barramento de Serviços do Processo Eletrônico Nacional (PEN).

Art. 6º As instâncias de SPED são compostas essencialmente por máquinas virtuais (VM) correspondentes aos servidores dedicados para cada OM, mantidas nos Centros de Telemáticas (CT) e nos Centros de Telemática de Área (CTA) e, quando estritamente necessário (por reais impossibilidades de redes ou afins), nas próprias OM.

Art. 7º A instância do MI será instalada em *cluster*, gerenciado pelas equipes de desenvolvimento e sustentação de sistemas do Centro de Desenvolvimento de Sistemas (CDS) e mantida na infraestrutura provida pelo 7º CTA. (figura 1).

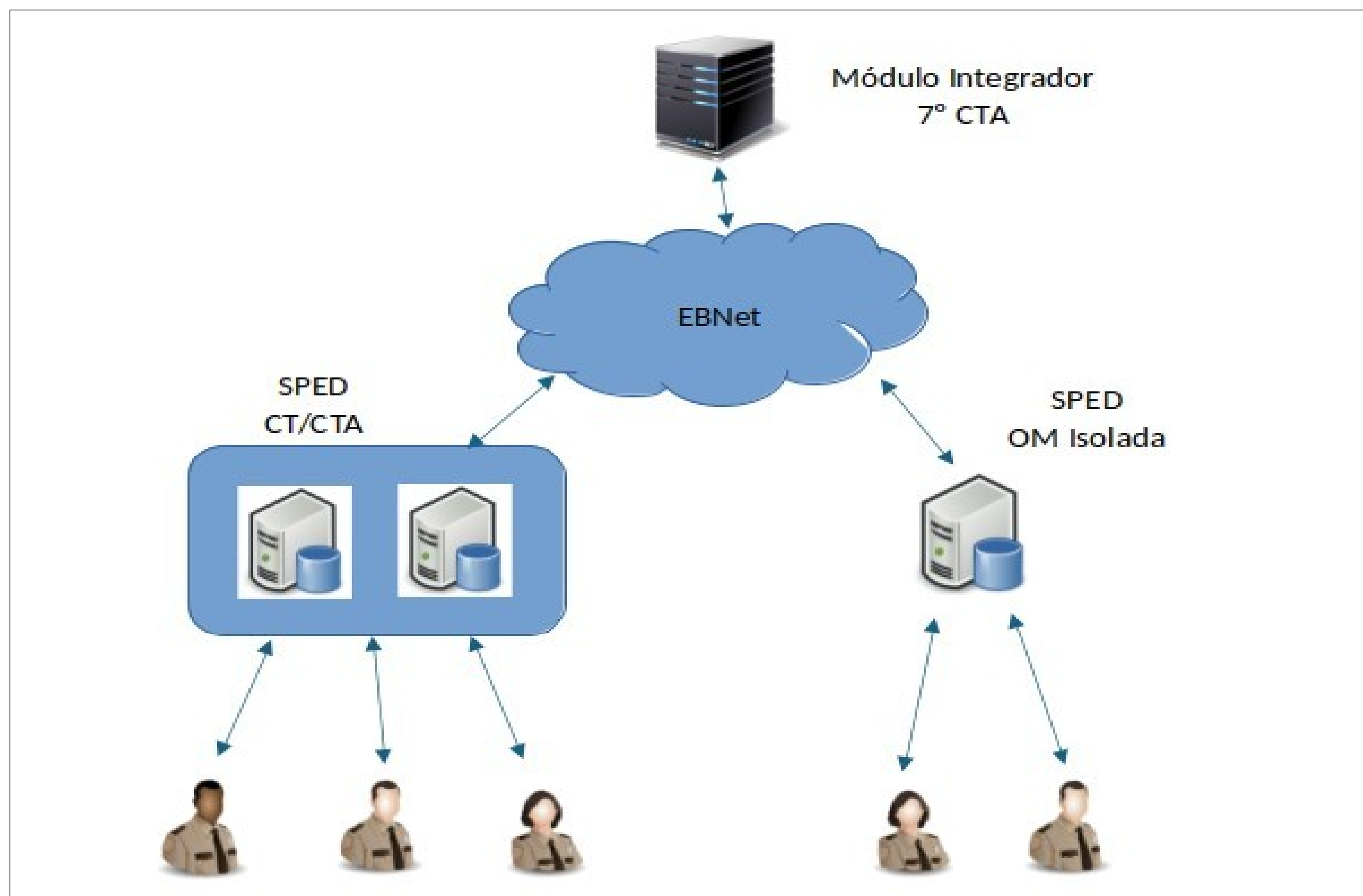


Fig 1 – Arquitetura do SIGADEx

Seção II
Da estrutura do sistema

Art. 8º Os órgãos abrangidos pelo SIGADEx em termos tecnológicos são organizados em 3 (três) níveis:

I - nível A: composto por unidades normatizadoras;
II - nível B: composto por unidades técnicas de suporte e manutenção; e
III - nível C: composto por unidades de produção.

§ 1º As unidades normatizadoras são compostas pelo Estado-Maior do Exército (EME), Órgão de Direção Geral (ODG) do EB, e o Departamento de Ciência e Tecnologia do Exército (DCT).

§ 2º As unidades técnicas de suporte e manutenção são compostas pelo Centro de Desenvolvimento de Sistemas (CDS) e o Centro Integrado de Telemática do Exército (CITEx), com seus CT/CTA.

§ 3º As unidades de produção são compostas por todas as OM do EB.

Seção III
Das atribuições

Art. 9º O EME é o órgão que regulamenta o acesso das organizações militares ao sistema informatizado de gestão documental por meio do fornecimento do Código de Organização

Militar (CODOM) e da faixa de número único de protocolo (NUP), dados essenciais para o credenciamento das instâncias do SPED no sistema.

Art. 10. O DCT é o órgão de direção setorial responsável por coordenar e aperfeiçoar a gestão dos sistemas e infraestrutura componentes do SIGADEx. Como órgão diretor de tecnologia da informação (TI), tem as seguintes atribuições:

I - propor ao EME a atualização da política e da diretriz de utilização do software do EB;

II - orientar e coordenar as atividades da gestão técnica do SIGADEx no âmbito do EB por meio de suas Organizações Militares Diretamente Subordinadas (OMDS) envolvidas no sistema;

III - gerenciar a governança técnica do sistema informatizado de apoio à gestão documental;

IV - orientar o suporte técnico na utilização das ferramentas informatizadas do SIGADEx;

V - orientar a manutenção do sistema informatizado de apoio à gestão documental em operação, visando ao seu contínuo aprimoramento; e

VI - contribuir nas ações de prospecção que possibilitem a criação ou aquisição de um repositório arquivístico digital confiável (RDC-Arq) em todos os níveis, bem como sua manutenção, objetivando a preservação dos dados digitais ou digitalizados no âmbito do EB.

Art. 11. O Centro Integrado de Telemática do Exército (CITEx) é o órgão do DCT responsável pela gestão da infraestrutura de telemática (hardware) no âmbito do Exército Brasileiro. Sua atribuição é realizar a coordenação da atuação dos CT/CTA em proveito do SIGADEx.

Art. 12. Os CT/CTA são as OM responsáveis pela operação dos meios de telemática que suportam o SIGADEx, envolvendo a conectividade dos usuários da OM às respectivas instâncias de SPED, tendo as seguintes atribuições:

I - ser, prioritariamente, o hospedeiro das instâncias de SPED das OM apoiadas;

II - ser o primeiro nível de suporte ao usuário do sistema;

III - ser o responsável pela execução de procedimento de *backups* das bases de dados, instalação e configuração das instâncias de SPED das OM apoiadas. Tais procedimentos devem seguir a orientação do CDS;

IV - prover o acesso aos usuários das OM aos softwares do sistema de gestão documental do Exército;

V - ser o responsável pela proteção cibernética dos meios de telemática envolvidos em apoio ao sistema de gestão de documentos;

VI - prover o sistema para realização de chamados de suporte técnico em apoio às OM que operam o sistema; e

VII - auxiliar na prospecção para a concepção de um RDC-Arq a ser adotado no âmbito do EB.

Art. 13. O CDS, como órgão técnico de sistemas, tem as seguintes atribuições em sua área de responsabilidade:

I - exercer as atividades relacionadas à manutenção evolutiva e corretiva dos sistemas (software) do SIGADEx;

II - desenvolver os sistemas informatizados de apoio à gestão documental, conduzindo as respectivas evoluções corretivas e evolutivas necessárias;

III - auxiliar nas prospecções para a concepção de um RDC-Arq a ser adotado no âmbito do EB; e

IV - fornecer o suporte à instrução das ferramentas informatizadas de apoio à gestão documental, disponibilizando recursos de aprendizagem necessários à operação destas ferramentas, tais como manuais e meios audiovisuais.

Art. 14. As unidades de produção são responsáveis por:

I - operar as ferramentas computacionais de gestão arquivística nos documentos produzidos ou recebidos, cuja custódia lhes seja atribuída; e

II - enviar as demandas relacionadas à gestão técnica de suporte e manutenção aos respectivos CT/CTA, que são os responsáveis por sua instância de SPED.

CAPÍTULO III
DO DESENVOLVIMENTO, OPERAÇÃO E SUSTENTAÇÃO DO SISTEMA

Seção I
Da conceituação

Art. 15. A gestão do ciclo de vida de sistemas informatizados é o conjunto de procedimentos técnicos referentes à implantação, teste, operação, proteção, evolução, manutenção e desfazimento dos recursos de hardware e software. A este conjunto de procedimentos dar-se-á o nome de Desenvolvimento-Operação, ou DevOp.

Parágrafo único. A gestão do ciclo de vida das ferramentas informatizadas do sistema arquivístico e documental do Exército deve-se integrar por meio da esteira EB-DevOps, que corresponde às ferramentas e práticas adotadas pelo próprio EB para esta finalidade e cujo órgão responsável em gerir é o CDS.

Seção II
Dos objetivos

Art. 16. Os objetivos da gestão do sistema informatizado do SIGADEx pela esteira EB-DevOps são:

I - racionalizar e padronizar a produção e a utilização dos sistemas informatizados produzidos e recebidos em todas as OM do Exército;

II - controlar o fluxo para construção e disponibilização dos sistemas informatizados em produção; e

III - assegurar a conformidade dos produtos de sistemas informatizados com os princípios básicos da boa prática de engenharia de software.

Seção III
Das fases do desenvolvimento e operação

Art. 17. A esteira EB-DevOps compreende 2 (duas) fases:

I - fase do desenvolvimento: são as ações ligadas à gestão dos softwares em apoio à gestão documental. Se subdividem em: planejamento, codificação, construção e teste; e

II - fase de operações: são as ações ligadas à disponibilização em produção do sistema. São subdivididas em: disponibilização da versão atualizada, pela atualização do sistema; pela operação do usuário; e pelo monitoramento.

Parágrafo único. A proteção cibernética do sistema permeia as atividades ligadas a todas as etapas das fases de desenvolvimento e operação, sendo de responsabilidade de todos os atores em seus níveis e será descrita em seção própria.

Seção IV
Das fases do desenvolvimento

Art. 18. São 4 (quatro) as fases do desenvolvimento:

I - planejamento;

II - codificação;

III - construção; e

IV - teste.

§ 1º O planejamento é a atividade de levantamento dos requisitos funcionais do sistema. No caso do sistema de gestão documental, compete ao Departamento de Educação e Cultura do Exército (DECEx), por meio da Diretoria de Patrimônio Histórico e Cultural do Exército (DPHCEx) e do Arquivo Histórico do Exército (AHEx), a elaboração e seleção dos requisitos de negócio do sistema, cabendo ao CDS a concepção técnica sobre os requisitos não funcionais.

§ 2º A codificação, a construção e o teste são atividades eminentemente técnicas de transformação dos requisitos funcionais e não funcionais em componentes de software válidos e seguros. Estas atividades são de responsabilidade do CDS.

Seção V
Das fases da operação

Art. 19. São 4 (quatro) as fases da operação:

I – distribuição;

II - instalação e atualização;

III - operação; e

IV - monitoramento.

§ 1º. A distribuição é a atividade de submeter os artefatos de software em repositório para os gestores de sistema dos CT/CTA. Devido às características técnicas envolvidas, a distribuição é realizada de forma incremental, sendo executada por ferramentas computacionais próprias. Estas atividades são de responsabilidade do CDS.

§ 2º A instalação e atualização são as atividades de implementação das instâncias de SPED de cada OM nas máquinas virtuais. Estas atividades são de responsabilidade dos CT/CTA.

§ 3º A operação é a utilização da ferramenta de software para a gestão arquivística e documental do Exército. Também envolvem as configurações específicas necessárias ao enquadramento da estrutura organizacional da própria OM. Esta atividade é de responsabilidade de cada OM do EB.

§ 4º O monitoramento é a supervisão do uso das ferramentas computacionais do sistema de gestão arquivística e documental. Esta atividade tem a responsabilidade dividida em 3 (três) níveis:

I - nível 1: gestão da própria OM, com encargos de supervisão do credenciamento e elaboração dos procedimentos de acesso e utilização da ferramenta entre os usuários da organização;

II - nível 2: gestão do CT/CTA, com encargos de supervisão dos recursos de hardware, conexão (rede), manutenção e segurança de acesso aos ativos; e

III - nível 3: gestão do CDS, com encargos de supervisão dos códigos gerados. É exercida por meio da elaboração de testes unitários, de integração, de carga, de aceitação e segurança de software em ambiente de homologação.

Seção VI
Da proteção cibernética

Art. 20. A proteção cibernética é um componente essencial para garantir a segurança e integridade de sistemas informatizados. Trata-se do conjunto de medidas e práticas voltadas para a defesa contra ameaças cibernéticas, como ataques que comprometem o funcionamento do sistema e acessos não autorizados a documentos. Envolve a implementação de protocolos de segurança, criptografia, monitoramento contínuo e ações proativas para mitigar riscos.

Art. 21. São obrigações dos usuários:

I - adotar práticas seguras, como a criação de senhas robustas;

II - não compartilhar senhas nem permitir a sua gravação nos navegadores;

III - prevenir-se de ataque de engenharia social;

IV - acessar o sistema por meio de máquinas seguras, fazendo uso de Sistemas Operacionais (SO) e software de antivírus atualizados, ao utilizar redes privadas virtuais (VPN);

V - acessar o conteúdo disponível apenas para o seu perfil de uso, conforme a função que exerce; e

VI - informar imediatamente ao administrador do sistema acessos indevidos de sua conta.

Art. 22. São obrigações dos gestores do sistema nas OM:

I - implementar e supervisionar medidas de segurança, confeccionando políticas de acesso, realização de auditorias e manutenção de *backups* seguros, quando a instância estiver sob sua responsabilidade;

II - promover a formação constante da equipe e estarem preparados para responder eficientemente a incidentes, minimizando possíveis impactos; e

III - informar imediatamente ao administrador do CT/CTA apoiador qualquer violação de acessos indevidos à instância de sua responsabilidade.

Art. 23. São obrigações dos desenvolvedores:

I - adotar práticas de codificação segura;

II - realizar testes de segurança regularmente;

III - manter-se atualizados sobre as mais recentes ameaças cibernéticas;

IV - corrigir ou mitigar vulnerabilidades do sistema, mantendo a resistência do sistema ao longo do tempo; e

V - promover conexão segura e criptografada entre as instâncias de SPED e o MI, por meio de certificado SSL/TLS.

Art. 24. São obrigações dos administradores do sistema CT/CTA:

I - implementar rigorosa política de controle de acesso às VM, garantindo que apenas usuários autorizados tenham permissões adequadas;

II - monitorar de forma constante o tráfego de rede em busca de atividades suspeitas, utilizando ferramentas de detecção de intrusões;

III - manter um plano de contingência e recuperação; e

IV - realizar gestão de certificados SSL/TLS para acessos aos sistemas, provendo conexão segura entre a estação cliente e o servidor sob sua responsabilidade.

Seção VII
Das assinaturas

Art. 25. A assinatura eletrônica, ou assinatura simples, é um recurso disponibilizado pelo SIGADEx, por meio da qual se registra a autenticidade do documento em um determinado sistema. Requer, apenas, de senha cadastrada no sistema para a autenticação de documentos e processo produzidos pelo SPED. Equivale ao nível descrito no inciso I do art. 4° do Decreto Presidencial n° 10.543, de 13 de novembro de 2020.

Art. 26. A assinatura digital, ou assinatura eletrônica qualificada, é um recurso disponibilizado pelo SIGADEx, prestando a realizar a autenticação e integridade de documentos e processos produzidos pelo SPED, segundo o padrão ICP-Brasil. Este tipo de assinatura é provido por mecanismo de Certificação Digital apropriado que estabelece esta autenticação do registro de fonte digital de forma ampla, bem como permite a validação de autenticidade e integridade do registro digital

por meio do validador do Instituto Nacional de Tecnologia da Informação (ITI). Equivale ao nível descrito no inciso III do art. 4º Decreto Presidencial nº 10.543, de 13 de novembro de 2020.

§ 1º O SPED atualmente implementa o uso da Certificação Digital do tipo A3 para assinatura digital, também chamada de assinatura eletrônica qualificada. Este tipo de certificado atende a padrões específicos e requisitos de segurança estabelecidos pela Autoridade Certificadora (AC), ligada às instituições de Defesa.

§ 2º O certificado digital A3 é uma classe de certificados que armazena chaves criptográficas em um dispositivo físico, como um cartão inteligente ou *token* USB. No contexto da Defesa, essa modalidade oferece um nível mais elevado de segurança em comparação com certificados digitais armazenados em mídias mais simples (A1). O "A3" sugere a forma física do dispositivo utilizado para armazenar as chaves criptográficas.

Art. 27. Os usuários que preencherem os requisitos poderão solicitar a geração de um Certificado Digital A3 vinculado à Defesa junto às Autoridades Certificadoras (AC) específicas designadas para esse propósito. A relação de unidades cadastradas poderá ser consultada no sítio da Internet relacionado, conforme processo estabelecido pela entidade.

Art. 28. Os usuários possuidores do Certificado AC/Defesa são responsáveis por gerenciar e fazer a guarda de suas credenciais, respondendo por sua utilização no sistema do SPED.

Parágrafo único. Para a utilização do Certificado A3, o usuário deve seguir as orientações recomendadas pelo CDS, incluindo fazer uso somente de sistemas indicados por este Órgão, disponíveis nos meios de instruções distribuídos.

Seção VIII
Da digitalização de documentos físicos

Art. 29. A digitalização de documentos é o processo de converter documentos em formato físico, como papel, em arquivos digitais. É realizada por meio de *scanners* ou outros dispositivos de digitalização, que capturam uma imagem do documento e a transforma em um arquivo eletrônico, geralmente em formato PDF, JPEG ou outro formato de imagem. Esses arquivos digitais podem então ser armazenados, organizados e acessados por meio de computadores ou sistemas de gerenciamento de documentos eletrônicos.

§ 1º Para fins de digitalização de arquivos de teor documental a serem protocolados no SIGADEx, fica estabelecido que os arquivos externos deverão ser importados em formato .PDF de digitalização OCR (*Optical Character Recognition*).

§ 2º Admite-se a digitalização de documentos em outros formatos quando não se aplicarem as razões previstas nas recomendações contidas no acórdão 389/2020 - TCU - Plenário, sobre disponibilização de inteiro teor dos processos eletrônicos que documentam as licitações e execuções de contratos por parte dos órgãos da Administração Pública que estão sob sua supervisão.

CAPÍTULO IV
DO REPOSITÓRIO DIGITAL CONFIÁVEL

Seção I
Da conceituação

Art. 30. O repositório digital confiável é um sistema ou plataforma que armazena e gerencia informações de forma segura, confiável e durável ao longo do tempo. É projetado para preservar a integridade, autenticidade e acessibilidade de dados digitais, garantindo que estes permaneçam disponíveis e utilizáveis ao longo do tempo, mesmo diante de mudanças tecnológicas ou ameaças potenciais.

§ 1º O repositório é projetado para garantir a preservação a longo prazo dos dados digitais, utilizando práticas como a migração de formatos e a atualização de metadados para acompanhar as mudanças tecnológicas.

§ 2º Mecanismos de controle são implementados para garantir a autenticidade e integridade dos dados armazenados. Pode envolver a utilização de assinaturas digitais, *hashs* integridade ou outros métodos para verificar se os dados não foram alterados ou comprometidos. São acompanhados por procedimentos robustos de *backup* e recuperação para garantir a disponibilidade dos dados, mesmo em caso de falhas.

Seção II
Do planejamento para a implantação

Art. 31. O EME, por meio do DECEx e DCT, expedirá orientação para a execução de trabalhos de prospecção de novas tecnologias no sentido de buscar implementar no âmbito do Exército um sistema de repositório confiável em complemento aos sistemas já em produção. Para tanto, por se tratar de um produto de alta complexidade, deve-se considerar que a atividade em questão poderá ser realizada por meio de aquisição ou desenvolvimento de uma solução compatível.

Parágrafo único. Por se tratar de um produto de alta complexidade, a concepção de uma solução de RCD-Arq poderá adotar, no processo de sua implementação, os mesmos conceitos previstos nas Instruções Gerais Para Gestão do Ciclo de Vida dos Sistemas e Materiais de Emprego Militar (EB10-IG-01.018).

GLOSSÁRIO

Assinatura digital - modalidade de assinatura eletrônica, resultado de uma operação matemática, que utiliza algoritmos de criptografia e permite aferir, com segurança, a origem e a integridade do documento. Os atributos da assinatura digital são: a) ser única para cada documento, mesmo que o signatário seja o mesmo; b) comprovar a autoria do documento digital; c) possibilitar a verificação da integridade; e d) assegurar ao destinatário o "não repúdio" do documento digital, uma vez que, a princípio, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura.

Assinatura eletrônica - geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser o laço legalmente equivalente à assinatura manual do indivíduo.

Autenticação - 1. Atestação de que um documento é verdadeiro ou de que uma cópia reproduz fielmente o original, de acordo com as normas legais de validação. 2. Declaração de que um documento original é autêntico – ou que uma cópia reproduz fielmente o original – feita por uma pessoa jurídica com autoridade para tal (servidor público, notário, autoridade certificadora) num determinado momento, por meio da adição de elementos ou afirmações.

Autoridade certificadora - organização que emite, renova ou revoga certificados digitais de outras autoridades certificadoras ou de titulares finais.

Banco de dados (ambiente computacional) - 1. Conjunto de dados relacionados entre si, estruturados em forma de base de dados, gerenciado por programa específico. 2. Ambiente computacional composto por: a) dados estruturados em bases de dados relacionadas entre si, segundo um modelo de dados; e b) regras que definem as operações válidas sobre os dados e garantem sua integridade.

Base de dados - conjunto de dados estruturados, com as respectivas regras de acesso, formatação e validação, e gerenciados por um Sistema Gerenciador de Banco de Dados – SGBD.

Certificação digital - atividade pela qual se estabelece uma relação única, exclusiva e intransferível entre um elemento criptográfico e uma pessoa física ou jurídica.

Certificado digital - registro eletrônico assinado, gerado por meio de um procedimento de certificação digital, que se destina a comprovar a relação existente entre um elemento criptográfico e uma pessoa física ou jurídica.

Chave privada - chave matemática formada por uma sequência de dígitos, usada para criptografia assimétrica e criada em conjunto com a chave pública correspondente que deve ser mantida em segredo pelo portador. Usada para assinar digitalmente documentos, bem como para decifrar aqueles criptografados com a chave pública correspondente.

Chave pública - chave matemática formada por uma sequência de dígitos, usada para criptografia assimétrica, criada em conjunto com a chave privada correspondente, disponibilizada publicamente por certificado digital e utilizada para verificar assinaturas digitais. Também pode ser usada para criptografar mensagens ou arquivos a serem decifrados com a chave privada correspondente.

Criptografia - método de codificação de dados segundo algoritmo específico e chave secreta, de forma que somente os usuários autorizados possam restabelecer sua forma original.

Criptografia de chave pública - tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais. Também chamada de criptografia assimétrica.

Gerenciamento eletrônico de documentos (GED) - conjunto de tecnologias utilizadas para organização da informação não estruturada de um órgão ou entidade, que pode ser dividido nas seguintes funcionalidades: captura, gerenciamento, armazenamento e distribuição. Entende-se por informação não estruturada aquela que não está armazenada em banco de dados, como mensagem de correio eletrônico, arquivo de texto, imagem ou som, planilhas etc.

Hardware - conjunto dos componentes físicos necessários à operação de um sistema computacional.

Infraestrutura de chaves públicas (ICP) - conjunto de técnicas, práticas e procedimentos que estabelecem os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública. Normalmente, é composto por uma cadeia de autoridades certificadoras formada pela autoridade certificadora raiz – AC Raiz, pelas demais autoridades certificadoras – AC e pelas autoridades de registro – AR.

Repositório arquivístico digital - repositório digital que armazena e gerencia documentos arquivísticos, seja nas fases corrente e intermediária, seja na fase permanente.

Repositório digital - plataforma tecnológica que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de *hardware*, *software* e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos.

Repositório digital confiável (RDC) - repositório digital que é capaz de manter autênticos, preservar e prover acesso a materiais digitais pelo tempo necessário.

Sistema de gestão arquivística de documentos - conjunto de procedimentos e operações técnicas cuja interação permite a eficiência e a eficácia da gestão arquivística de documentos. Ver também: gestão arquivística de documentos; sistema informatizado de gestão arquivística de documentos.

Sistema de Protocolo Eletrônico de Documentos (SPED) sistema responsável pelo protocolo e confecção de documentos das OM do EB.

Sistema gerenciador de banco de dados (SGBD) - *software* que implementa o banco de dados e permite a realização de operações de manipulação de dados (inclusão, alteração, exclusão, consulta) e administrativas (gestão de usuários, cópia e restauração de dados, alterações no modelo de dados).

Sistema informatizado - sistema que apoia o acesso e a gestão de dados, informação e/ou documentos em um sistema computacional.

Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) - 1. Sistema desenvolvido para produzir, receber, armazenar, dar acesso e destinar documentos arquivísticos, sejam os documentos convencionais ou os digitais, convencionais e dinâmicos, inclusive páginas web e bancos de dados. As ações do SIGAD aplicam-se a documentos convencionais, ao registrar suas referências, podendo, ainda, incorporar imagens digitalizadas dos documentos. Aplicam-se, ainda, aos documentos digitais, através de sua captura, armazenamento e promoção de acesso. O SIGAD poderá ser composto por *software* único ou vários *softwares* integrados, adquiridos ou encomendados. Seu sucesso dependerá da implantação prévia de um Programa de Gestão Arquivística de Documentos. 2. Conjunto de procedimentos e operações técnicas característico do sistema de gestão arquivística de documentos processado eletronicamente e aplicável em ambientes digitais ou em ambientes híbridos, isto é, documentos digitais e não digitais ao mesmo tempo.

Sistema Informatizado de Gestão Arquivística e Documental do Exército (SIGADEx) - é um sistema informatizado de gestão arquivística de documentos do EB.

Software - é o conjunto de instruções lógicas e dados que permitem que um sistema de computador execute tarefas específicas.